



## **Reflected Signal Analysis**

**by Deen King-Smith, Anthony Martone, and Marc Ressler**

---

**ARL-TR-5054**

**January 2010**

## **NOTICES**

### **Disclaimers**

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

# **Army Research Laboratory**

Adelphi, MD 20783-1197

---

---

**ARL-TR-5054**

**January 2010**

---

## **Reflected Signal Analysis**

**Deen King-Smith, Anthony Martone, and Marc Ressler**  
**Sensors and Electron Devices Directorate, ARL**

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>					
1. REPORT DATE (DD-MM-YYYY) January 2010		2. REPORT TYPE Final		3. DATES COVERED (From - To) May to September 2009	
4. TITLE AND SUBTITLE Reflected Signal Analysis				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Deen King-Smith, Anthony Martone, and Marc Ressler				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory ATTN: RDRL-SER-U 2800 Powder Mill Road Adelphi, MD 20783-1197				8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-5054	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT We present a framework for forensic identification of RF devices using specially designed probe signals. This framework applies to a broad range of devices and models. Probe signals, device models, feature selection, and classifier design are described. For the device model, we introduce a method for determining a nonlinearity based on a known diode model. Experimental results are given to verify our approach.					
15. SUBJECT TERMS Waveform design, filter analysis, diode modeling, RF circuit characterization, feature extraction, pattern recognition					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 32	19a. NAME OF RESPONSIBLE PERSON Anthony Martone
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include area code) (301) 394-2531

---

## Contents

---

<b>List of Figures</b>	<b>iv</b>
<b>List of Tables</b>	<b>iv</b>
<b>Acknowledgments</b>	<b>v</b>
<b>1. Introduction</b>	<b>1</b>
<b>2. Probe Signal Design</b>	<b>2</b>
2.1 Linear Chirp .....	2
2.2 Gaussian Windowed Chirp.....	3
<b>3. Experiment 1</b>	<b>5</b>
3.1 Shockley Diode Model .....	8
3.2 Experiment .....	9
<b>4. Experiment 2</b>	<b>13</b>
4.1 Probe Signal .....	13
4.2 Device Model .....	13
4.3 Reflected Response .....	14
4.4 Feature Selection .....	15
4.5 NCSU Experimental Set up.....	15
4.6 Experimental Set up .....	18
<b>5. Future Work</b>	<b>20</b>
<b>6. References</b>	<b>21</b>
<b>List of Symbols, Abbreviations, and Acronyms</b>	<b>22</b>
<b>Distribution List</b>	<b>23</b>

---

## List of Figures

---

Figure 1. System block diagram. ....	1
Figure 2. Sample linear chirp signal. ....	3
Figure 3. Sample time domain Gaussian chirp. ....	4
Figure 4. Circuit model for Experiment 1.....	5
Figure 5. Sample power spectrums of the return signal from each model. ....	7
Figure 6. Diode response curves. ....	10
Figure 7. Power spectral density (PSD) of nonlinear model. Nonlinear model uses coefficients estimated from the diode response curves.....	10
Figure 8. Plot of results. ....	12
Figure 9. Block diagram of a typical RF front-end.....	13
Figure 10. Simplified RF front-end. ....	14
Figure 11. Example reflected filter response of a back-to-back linear chirp probe signal. ....	14
Figure 12. Sampling the filter reflected response. ....	15
Figure 13. Experimental measurement system. ....	16
Figure 14. Frequency spectrum of excitation probe. ....	17
Figure 15. Frequency spectrum of mapped excitation.....	17
Figure 16. Result from SVM classifier segmented by SNR. ....	18

---

## List of Tables

---

Table 1. Parameters used for Gaussian chirp.....	5
Table 2. Gaussian chirp signal parameters. ....	6
Table 3. Parameters used in each circuit model for the Gaussian chirp simulations.....	6
Table 4. Shockley diode parameters. ....	9
Table 5. Resulting classification accuracies determined by the SVM for Experiment 1. ....	12
Table 6. Resulting classification accuracies determined by the SVM for Experiment 2. ....	19

---

## Acknowledgments

---

We wish to thank Karl Kappra, Francois Koenig, and John Costanza for guidance during the course of this project and assistance with configuration of lab equipment. We would also like to thank Dan Haugh for the initial suggestion of the Shockley diode model.

INTENTIONALLY LEFT BLANK.



---

## 1. Introduction

---

Wireless devices are ubiquitous. Forensic characterization of a wireless device is useful in many applications. An example of this is in the testing of Federal Communications Commission (FCC) Part 15 devices (1). These devices must adhere to strict guidelines with regard to RF interference; one reason being problems with Portable Electronic Devices (PEDs) carried on board aircraft. Title 14 of the Code of Federal Regulations (14 CFR) §§ 91.21, 121.306, 125.204, and 135.144 limits the operation of PEDs aboard U.S.-registered civil aircraft. These rules also permit the use of specific PEDs after the aircraft operator has determined that the PED will not interfere with the operations of the aircraft (2). However, how can the aircraft operator know which PEDs are approved, or if the approved devices are being operated at inappropriate times (3)? Compliance can be verified by detecting the operation of transmitting PEDs (T-PEDs) using an onboard monitoring system (4) or it could be verified by characterizing the device at a gate entry point, whether powered on or off, using specially designed probe signals and using forensic techniques to classify the returned signal. In a more general setting, forensic characterization allows determination of the type of device, make, model, configuration, and other characteristics based on observation of the data that the device produces. The unique characteristics of the device are known as device signatures or device fingerprints.

To characterize an RF device, the device is excited using a specially designed probe signal. The probe signal interacts with several circuit components, each of which modifies the probe signal, effectively embedding information into the signal. The embedded information is unique to each circuit component. The modified signal is then transmitted from the device and captured by a receiver. Features, or key characteristics, are extracted from the received signal and formed into a feature vector. The feature vector forms the device signature or device fingerprint that is then characterized using a classification system. A block diagram of the general system is shown in figure 1.

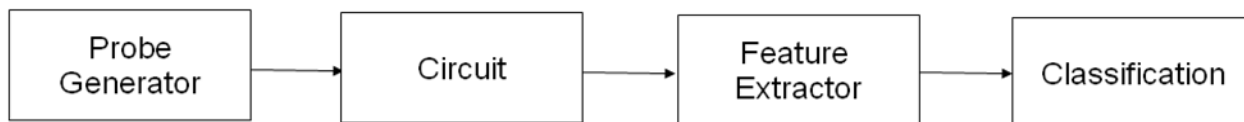


Figure 1. System block diagram.

In this report, we enhance our waveform and modeling design from two previous experiments. Experiment 1 used a linear chirp signal multiplied by a Gaussian window to excite a nonlinear system model. This experiment focused on mathematical modeling of the system response and classification methods using five combinations of filters and nonlinear components. This work was based on thesis work by Anthony Martone (5) at Purdue University. We extend this research

by developing a model for the nonlinearity based on a diode and perform a comprehensive analysis of all possible combinations (not limited to five) of the filter and nonlinearity at several different noise levels.

Experiment 2 used a linear chirp to excite the system with a focus on large bandwidth filter responses without the presence of a nonlinearity. This experiment, initially conducted by Purdue University and North Carolina State University (NCSU), encountered several hardware limitations that restricted the bandwidth of the probe to 100 MHz. To overcome this limitation the measured reflected responses were mapped to a larger response prior to feature selection and analysis. For this experiment, we capture the response to a large bandwidth signal for analysis and add a diode to act as a nonlinearity in the system. This alleviates the need for mapping.

---

## 2. Probe Signal Design

---

### 2.1 Linear Chirp

The probe signal  $p(t)$  used in both experiments is based on a linear chirp. Chirp signals are attractive because they allow the probe signal to have a large bandwidth and low peak transmission power. The frequency content of the probe may then generate more information that can be used to characterize the circuit. This type of chirp was originally chosen to enable estimation of the center frequency of the excited filter using only simple time domain features, as will be described in the following sections. The characteristics of this probe are appropriate for the device model employed here, which focuses on the reflected response of a linear bandpass filter. The linear chirp is defined as

$$l(t) = C \cos(\phi) \tag{1}$$

with  $\Phi$  defined as

$$\phi(t) = 2\pi f_0 t + \pi k t^2 \tag{2}$$

where

- $C$  is the amplitude of the signal
- $t$  is the time variable
- $f_0$  is the frequency at  $t=0$
- $k$  is the chirp rate

The instantaneous frequency is defined as

$$\dot{\phi}(t) = 2\pi f_0 + 2\pi kt \quad (3)$$

An example of this signal is shown in figure 2.

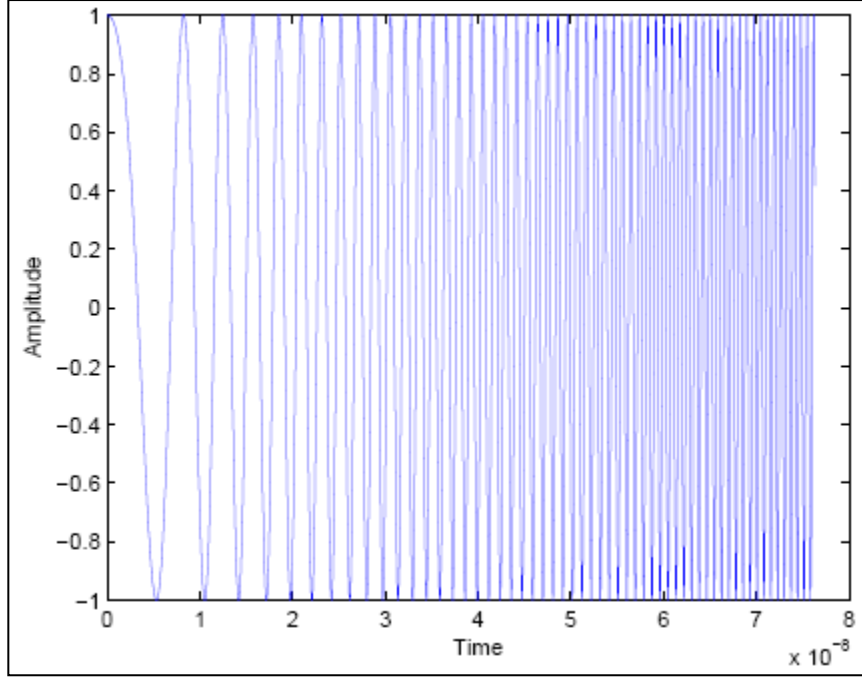


Figure 2. Sample linear chirp signal.

## 2.2 Gaussian Windowed Chirp

For Experiment 1, we designed a probe signal that is windowed by a Gaussian function. This is done by multiplying the linear chirp signal by a Gaussian window function in the time domain. The Gaussian window function is used since it generates a wide main lobe and produces rapidly decaying side lobes in the frequency domain (6). The Gaussian window function is described in the form of a Gaussian envelope:

$$w(t) = e^{\frac{-(t-\mu)^2}{2\sigma^2}} \quad (4)$$

where

$$\mu = \int_{-\infty}^{\infty} tw(t)dt \quad (5)$$

and

$$\sigma^2 = \int_{-\infty}^{\infty} (t - \mu)^2 w(t) dt > 0 \quad (6)$$

The windowed linear chirp, which we refer to as the Gaussian windowed chirp, is then formed  $x(t) = w(t)l(t)$ . Thus,  $x(t)$  is

$$x(t) = C_1 e^{i\phi(t)} e^{-\frac{(t-\mu)^2}{2\sigma^2}} \quad (7)$$

An example of  $x(t)$  (real part) is shown in figure 3. The parameters used to generate this signal are shown in table 1.

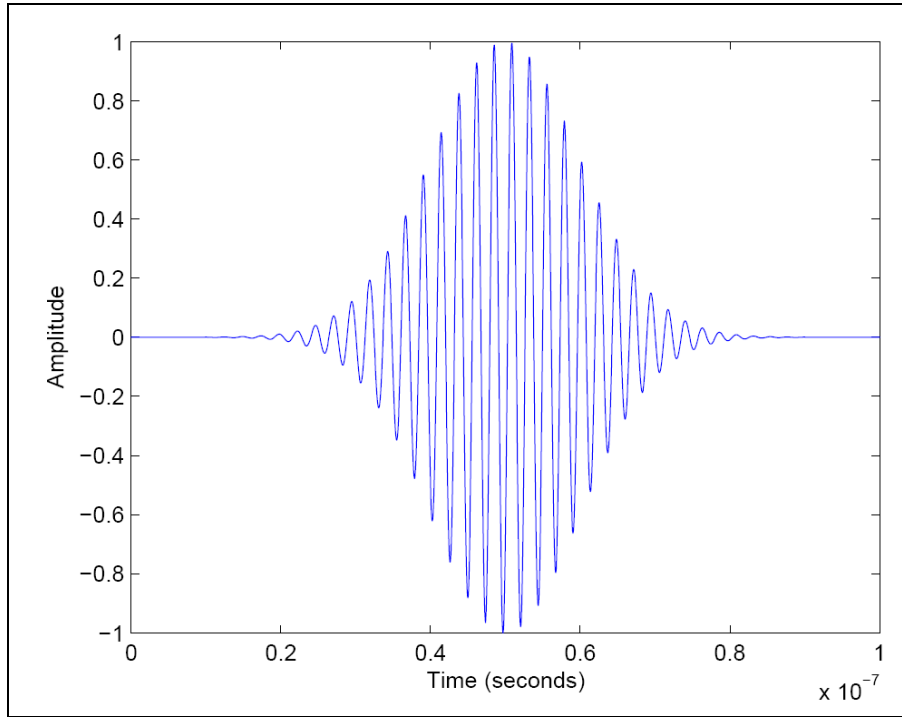


Figure 3. Sample time domain Gaussian chirp.

Table 1. Parameters used for Gaussian chirp.

Parameter	Description	Value
$C_1$	Amplitude of signal	1
$i$	Imaginary number	$\sqrt{-1}$
$f_0$	Initial frequency at $t = 0$	400MHz
$f_1$	Final frequency at time $t_1$	450MHz
$t_1$	Final time	$0.1 \times 10^{-6}$
$k$	Chirp rate	$5 \times 10^{14}$
$\mu$	Mean	$5 \times 10^{-8}$
$\sigma$	Standard deviation	$1 \times 10^{-8}$

### 3. Experiment 1

This experiment studies reflected signals resulting from a Gaussian windowed chirp exciting a combination of filter and nonlinearity models with noise added. Features were extracted from the reflected signals and then were classified using a set of known classifiers to compare the results. A block diagram of this system is shown in figure 4. The nonlinearity used in this system is modeled after a  $M=3$  order Taylor-series, the noise is Additive White Gaussian Noise (AWGN) at specific power levels, and the filters are 2<sup>nd</sup> and 4<sup>th</sup> order Chebyshev bandpass filters.

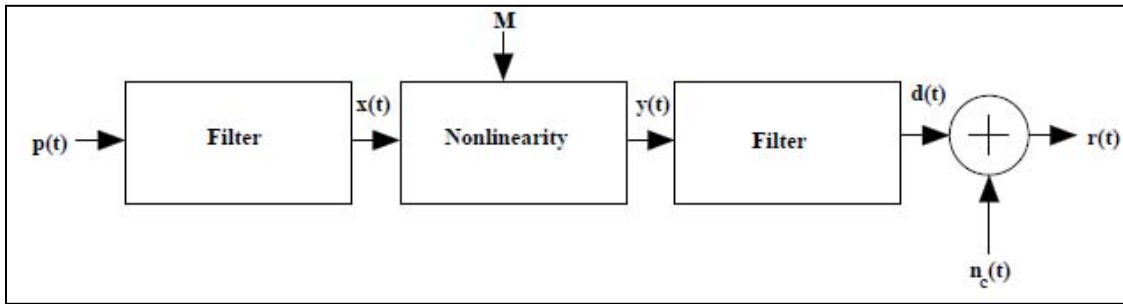


Figure 4. Circuit model for Experiment 1.

Five circuit models were used in this experiment. Each circuit model was excited with a Gaussian windowed chirp generated with the parameters found in table 2. Each nonlinearity parameter in the system is defined as  $a_i$ , which is the  $i^{\text{th}}$  coefficient in the Taylor-series. This specific parameter value was initially based of observations of an actual nonlinear response, with

additional values determined to elicit a specific response. The first four models have the parameters found in table 3, while the fifth represents the noise only case. Sample responses for each model can be found in figure 5.

Table 2. Gaussian chirp signal parameters.

Parameters	Description	Definition
$C_1$	Amplitude of signal	1
$i$	Imaginary number	$\sqrt{-1}$
$f_0$	Frequency at $t = 0$	1Hz
$f_1$	Frequency at $t_1$	2GHz
$t_1$	Final time	$50\mu s$
$t$	Time	$0 \leq t \leq 50\mu s$
$k$	Chirp rate	$4 \times 10^{13}$
$\mu$	Mean	$1.5 \times 10^{-5}$
$\sigma$	Standard deviation	$3.5 \times 10^{-6}$

Table 3. Parameters used in each circuit model for the Gaussian chirp simulations.

	$\Upsilon_1$	$\Upsilon_2$	$\Upsilon_3$	$\Upsilon_4$
$a_1$	0.01	0.001	0.003	0.007
$a_2$	0.008	0.0009	0.001	0.0009
$a_3$	0.009	0.00007	0.0007	0.00007
Filter Passband (MHz)	400-450	N/A	670-710	N/A
Filter Order	2	N/A	4	N/A

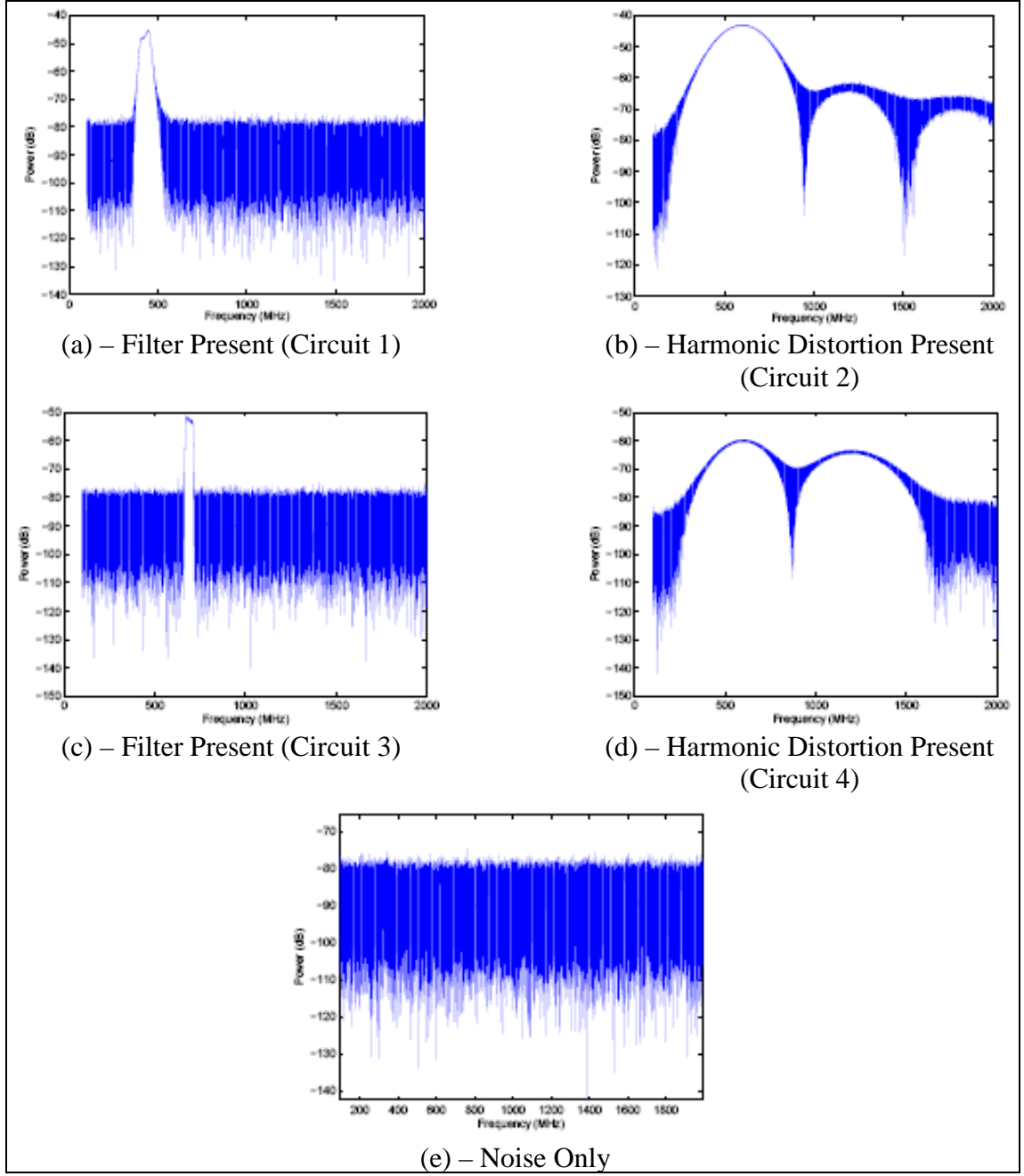


Figure 5. Sample power spectrums of the return signal from each model.

After the reflected signal is captured, white Gaussian noise, defined as  $n_{c_i}(t) \sim N(0, \sigma_{c_i}^2)$ , is added to the response, where  $i \in \{1, \dots, 5\}$  identifies the noise level in terms of the signal-to-noise ratio (SNR) referenced to the power of the input signal. The five added noise levels with respect to SNR are defined as  $\{-3.5137, -2.9580, -2.7889, -2.3987, \text{ and } -1.8417 \text{ dB}\}$  and are tested with each circuit model. In addition, we also test the noiseless response. This noise is added to

simulate system noise that represents possible variations between filters. Features are extracted from the power spectra of  $r(t)$  to create feature vectors. Each spectrum is sampled 34 times at regular intervals across a sampling range of 200–1900 MHz. The resultant feature vectors are used to form training and testing sets of data for the classifiers. In previous experimentation, the training and testing data were input into six types of classifiers to determine classification accuracy. These include Support Vector Machines (SVM), K-Nearest Neighbors (K-NN), Parzen Window (PW), Binary Tree (BT), and two types of Bayesian (BC) classifiers. The result showed that classification errors occur for features sampled from a power spectrum with a low SNR. The SVM, BT, PW, and K-NN classifiers had near perfect classification accuracies. In this report, we expand upon this research by developing a method for a more robust approach for selecting the parameters of the nonlinear models. Our approach for selecting the parameters is based on using the Shockley diode model.

### 3.1 Shockley Diode Model

The parameters of the nonlinear model (e.g.,  $a_1, a_2, \dots, a_M$ ) were chosen based on the Shockley ideal diode equation. This equation states

$$I = I_s \cdot (\exp(\frac{eV}{kT}) - 1) \quad (8)$$

where

- $I$  = current through diode
- $I_s$  = reverse saturation current
- $e$  = electron charge 1.602E-19 coulombs
- $V$  = applied voltage
- $K$  = Boltzmann's constant 1.389E-23
- $T$  = temperature in degrees Kelvin at 72 °F (295 K)

We used this equation to generate current versus applied voltage (I–V) curves, where the features of the curves characterized linear and nonlinear attributes of a diode for the selected parameters. The Shockley ideal diode equation is derived with the assumption that the only processes giving rise to current in the diode are drift due to electrical field, diffusion, and thermal recombination-generation (R-G). It also assumes that the R-G current in the depletion region is insignificant. This means that the Shockley equation does not account for the processes involved in reverse breakdown and photon-assisted R-G. Additionally, it does not describe the “leveling off” of the I–V curve at high forward bias due to internal resistance. Using this model, we repeated Experiment 1, replacing the original nonlinearity parameter values with ones calculated using the Shockley method.



### 3.2 Experiment

For our experiment, we looked at all possible combinations of the filter, nonlinearity, and noise levels. This included all possible permutations of the following:

- 5 nonlinearities
  - 4 diode-based nonlinearities
  - No nonlinearity present case
- 3 filters
  - 2 filters from table 3
  - No filter present case
- 6 noise values with 500 variations of each
  - 5 noise power values, as defined in section 3
  - No noise present case

These components were arranged in a way similar to that found in figure 4, and excited by a probe defined by equation 7 with the parameters found in table 2. These experimental parameters were identical to those found in table 3 with the exception of the nonlinearity parameters. For these parameters, we use the Shockley model described in section 3.1. Our input applied voltage (V) ranged from 0 to 1 V with steps in 0.01 V increments. The reverse saturation current ( $I_s$ ) was sourced from an Hewlett-Packard (HP) diode specs. Four of these parameters were used and are shown in table 4.

Table 4. Shockley diode parameters.

Diode	Source	$I_s$ (amps)
d1	HP	$1 \times 10^{-10}$
d2	HP HSCH-3171	$7 \times 10^{-8}$
d3	HP HSCH3486	$6 \times 10^{-6}$
d4	Common value	$1 \times 10^{-12}$

Using the Shockley diode parameters and the applied voltage range results in the curves shown in figure 6. The MATLAB function *Polyfit* was used to generate a set of coefficients that are then used for the Taylor-series representation of the nonlinearity. When excited by the Gaussian windowed chirp signal described in section 3, the spectrum response was similar to that found in figure 5b and 5d. A sample of this response is shown in figure 7.

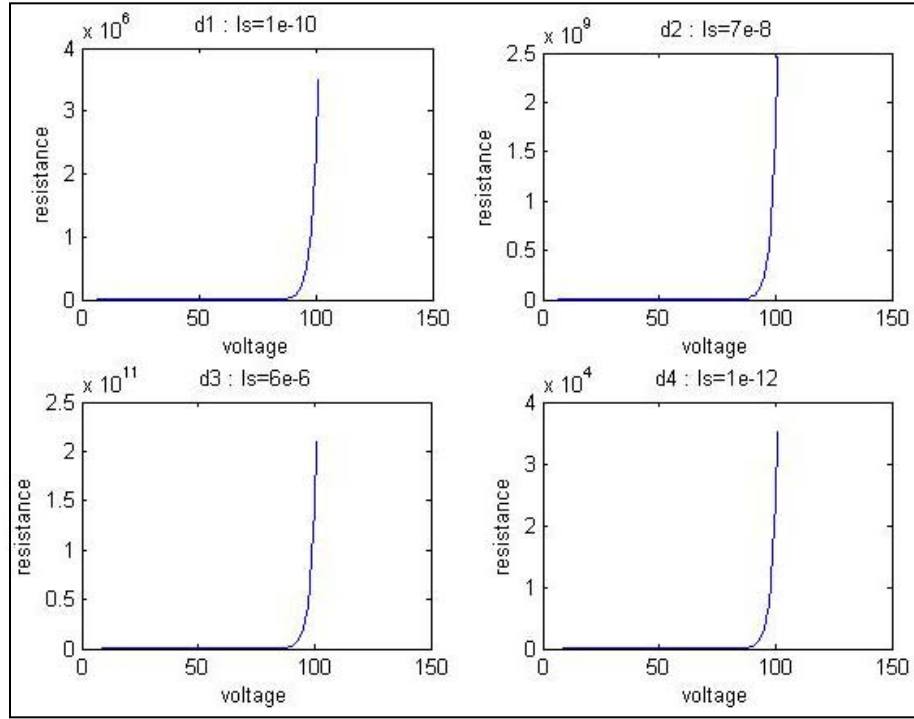


Figure 6. Diode response curves.

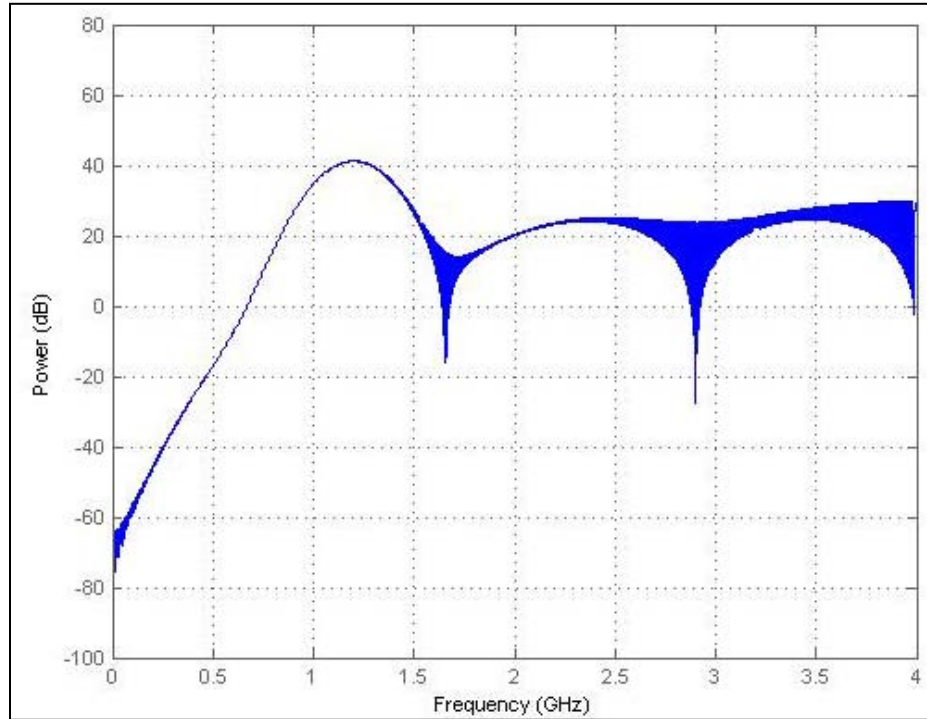


Figure 7. Power spectral density (PSD) of nonlinear model. Nonlinear model uses coefficients estimated from the diode response curves.

The diode response, as seen in figure 6, is almost identical between different values for  $I_s$ . The major difference here is in the amplitude of the response. The experiment generated a total of 45,000 responses, which included variations of 7 basic system responses:

- Nonlinearity + Filter + Noise (20,000 responses)
- Nonlinearity + Filter (4,000 responses)
- Nonlinearity + Noise (10,000 responses)
- Filter + Noise (5,000 responses)
- Filter only (1,000 responses)
- Nonlinearity only (2,000 responses)
- Noise only (2,500 responses)
- No noise + No filter + No nonlinearity (500 responses)

The variations differed based on the possible combinations of the input parameters to generate the combined 45,000 responses. From this system, we created three feature superset groups for analysis, which included the filter only, diode only, and filter + diode groups. Each class in the super set was based on the group delimiter, regardless whether or not another component was present. For example, the class for filter 1 in the filter only group included all responses where filter 1 was present. Similarly in the diode only case, each class contained a group of responses in which the particular diode was present. In the diode + filter case, each class contained the set of responses in which a particular filter/diode pair was present.

Specifically the filter 1 class contained responses from the following:

- Nonlinearity + Filter 1 + Noise (10,000 responses)
- Nonlinearity + Filter 1 (2,000 responses)
- Filter 1 + Noise (2,500 responses)
- Filter 1 only (500 responses)
- Nonlinearity only (2,000 responses)

Feature vectors were obtained by determining the power spectrum of each response and uniformly taking 34 samples from each response. For this analysis, we used the SVM (7) for our classification algorithm. This classifier is used due to its near perfect classification performance when compared to other classifiers (5). Each feature superset group was further broken down by noise power level. This was done to illustrate the affect of noise on classifier performance. The resulting classification accuracies generated by the SVM are shown in table 5 and figure 8.

Table 5. Resulting classification accuracies determined by the SVM for Experiment 1.

SNR (dBm)	Filter	Filter + Diode	Diode	Noise Power level
0	92.88%	44.85%	54.19%	0
-3.5137	91.04%	38.77%	45.73%	$5.00 \times 10^{-10}$
-2.9580	93.41%	49.98%	52.91%	$5.00 \times 10^{-9}$
-2.7889	92.21%	32.24%	53.49%	$1.00 \times 10^{-8}$
-2.3987	87.31%	32.24%	45.07%	$5.00 \times 10^{-8}$
-1.8417	86.75%	25.23%	45.07%	$5.00 \times 10^{-7}$

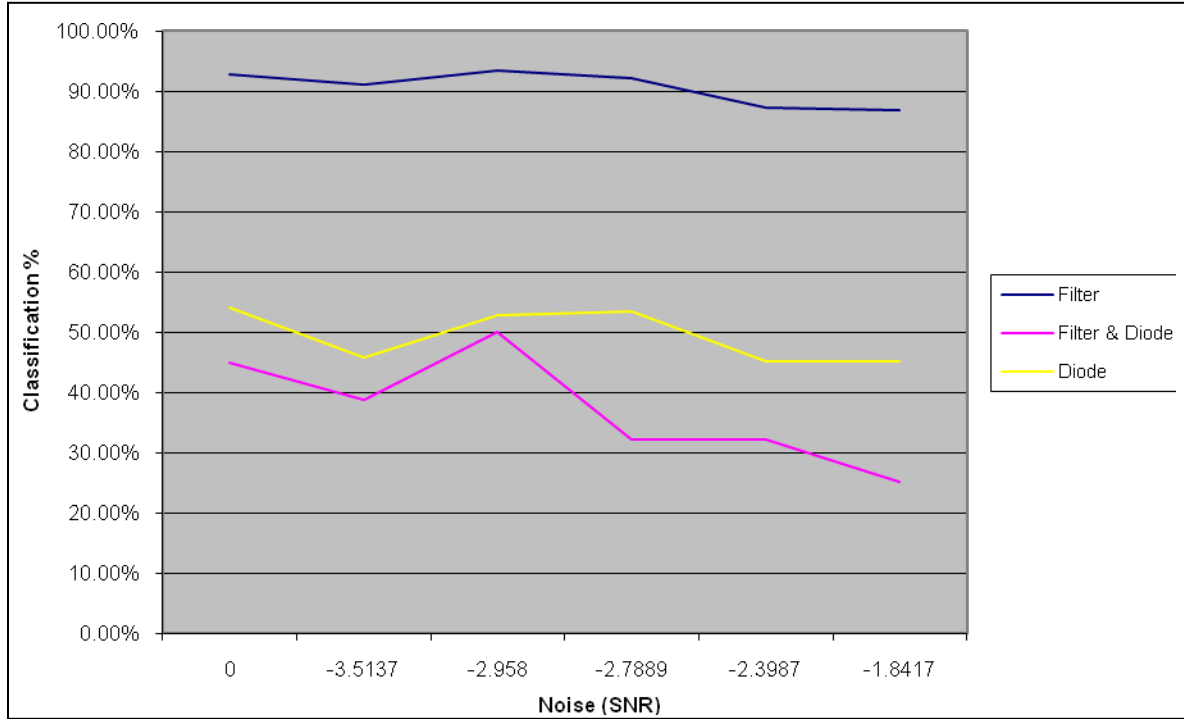


Figure 8. Plot of results.

From the results we can see that the filter appears to be the dominant feature. Note that the noiseless system did not produce a 100% classification accuracy, which was caused when the features extracted were scaled before being used by the classifiers since the pattern of the power spectrum of the nonlinearities was identical. This result warrants further investigation of the unscaled features. In addition, figure 8 illustrates that our classification accuracy did not monotonically decrease as the SNR decreased. This may be due to scaling effects introduced in the classifier or to other processes inherent in the model and calls for further investigation.

---

## 4. Experiment 2

---

The original experiment conducted by Purdue University and NCSU studied the reflected signal of a filter excited by a linear chip probe. This response was measured from a physical filter and noise was added using MATLAB. The initial goal was to capture a wideband reflected response of the filter (8). The spectrum analyzer allowed for only a 100 MHz wide measurement of the reflected response. To overcome this limitation the data were mapped to a synthetically generated larger response.

### 4.1 Probe Signal

The probe signal we used in this study was a back-to-back chirp, which was the same as defined in section 2.1; however, the instantaneous frequency was defined as

$$\dot{\phi}(t) = \begin{cases} 2\pi f_0 + 2\pi Kt, & 0 \leq t \leq T_p/2 \\ 2\pi f_1 + 2\pi K(T_p/2 - t), & T_p/2 \leq t \leq T_p \end{cases} \quad (9)$$

Here  $T_p$  is the length of the signal in seconds and  $K$  is the chirp rate in MHz/s. This chirp sweeps from  $f_0$  to  $f_1$  and back to  $f_0$ . This type of chirp was chosen to allow estimation of the center frequency of the excited filter using only simple time domain features.

### 4.2 Device Model

Typical RF devices contain a “front-end” circuit similar to that shown in figure 9, where the “front-end” is the circuitry between the antenna and the intermediate frequency (IF) section of the circuit. The probe signal is received by an antenna, passes through a bandpass filter, and is input into an amplifier.

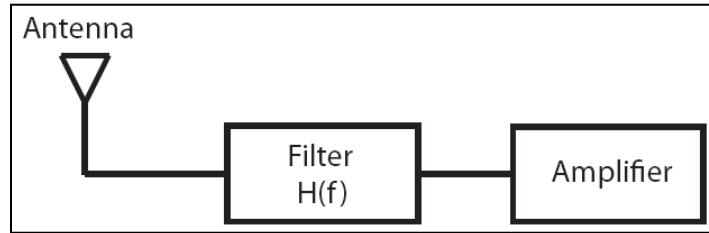


Figure 9. Block diagram of a typical RF front-end.

Typically, these three components are impedance matched, which allows us to simplify the front-end to the model, as shown in figure 10, where the only component of interest is the bandpass filter.

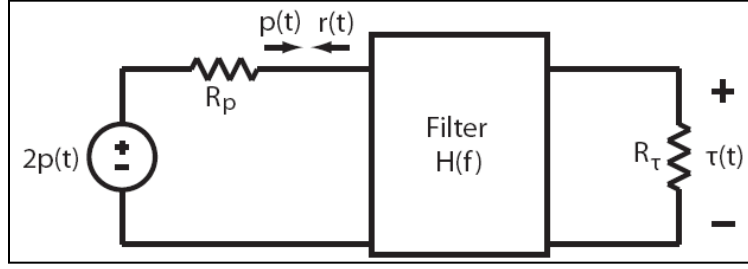


Figure 10. Simplified RF front-end.

This work focused on the filter modeled in figure 10. Specifically, these filters differed enough between devices that characterization of the filter itself provided enough information to characterize the device. The simplified front-end replaced the antenna with the signal source  $2p(t)$  in series with  $R_p$ , which was matched to the filter impedance. The node voltage between the filter and  $R_p$  was the sum of the signal  $p(t)$  and the reflected response  $r(t)$ . Similarly the filter was terminated with resistance  $R_t$ , which was also matched to the filter impedance.  $\tau(t)$  is the transmitted response of the filter; this signal was of no interest to us in the scope of this report.

### 4.3 Reflected Response

The filters to be characterized (i.e., those in typical RF devices) were assumed to be linear, time invariant, and bandpass with passbands within the frequency range of the probe signal, between  $f_0$  and  $f_1$ . Furthermore, since we were considering the filter response only, we modeled the input to the device as a filter with a matched load as shown in figure 10. When the probe signal excites the filter, a portion of the probe is reflected back from the filter and is called the reflected response. An example of this response is shown in figure 11.

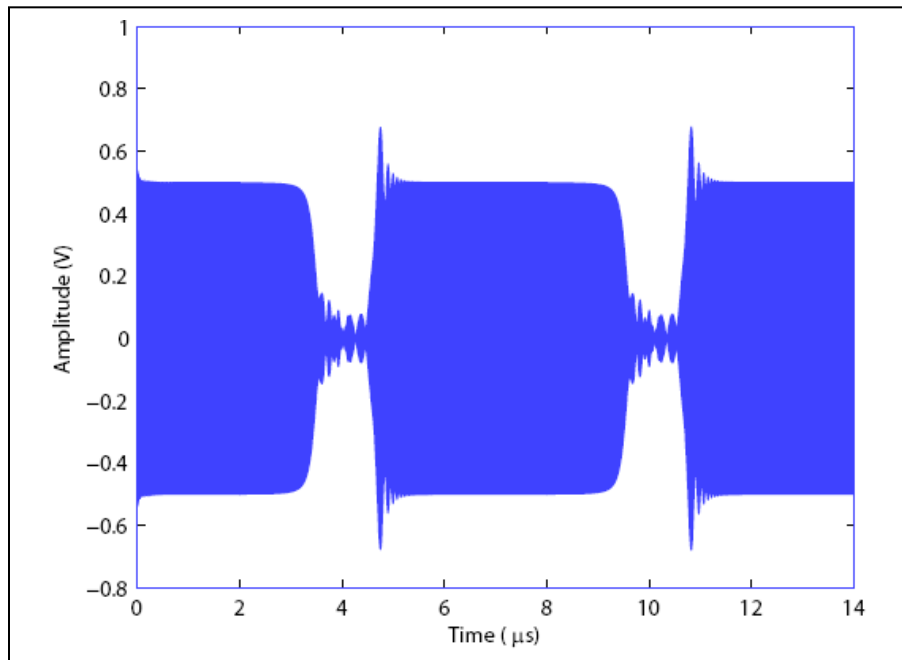


Figure 11. Example reflected filter response of a back-to-back linear chirp probe signal.

#### 4.4 Feature Selection

Several features were selected from the response. These features included the center frequency, bandwidth, and sampled passband of the excited filter. The “dips” in the response, seen in figure 11 and with more details in figure 12, were located in the passband of the filter, where the majority of the excitation signal passes through the filter, and did not contribute to the reflected response. Features were estimated from the envelope of the passband signal. To obtain the envelope of the reflected signal, it was passed through a square law device and low pass filter. Then, 36 features were obtained from this envelope. First, the center frequency of the filter was estimated from the envelope;  $ep,n[k]$  is found by estimating the sample indices corresponding to the cutoff frequencies of the passband, which in turn allows the bandwidth to be estimated. The remaining 34 features were sampled from the passband of the filter. An example of this is shown in figure 12.

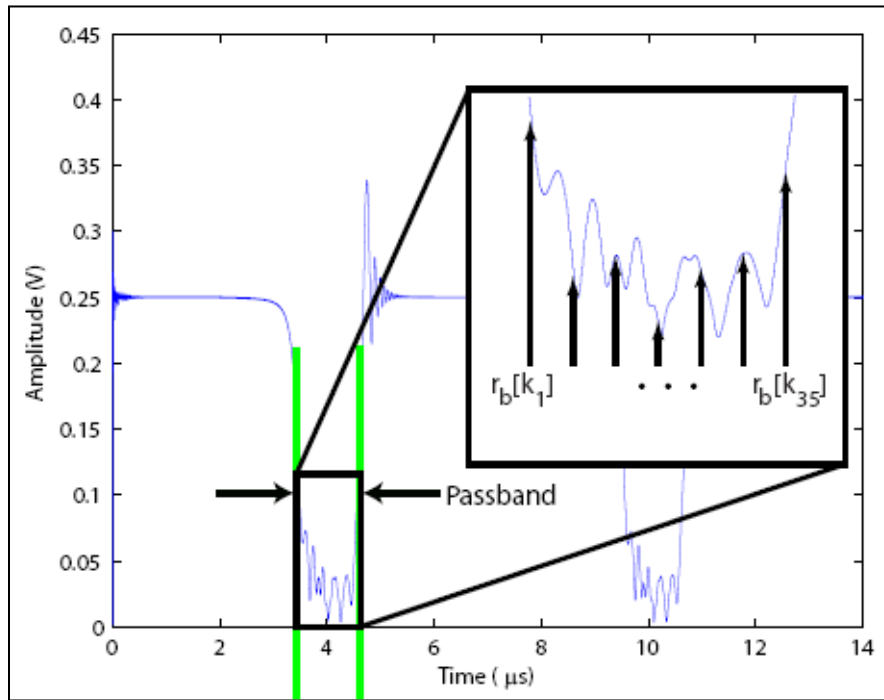


Figure 12. Sampling the filter reflected response.

#### 4.5 NCSU Experimental Set up

The original NCSU experiment used a probe signal that had  $f_0 = 100$  MHz,  $f_1 = 1000$  MHz,  $K = 120 \times 10^6$  MHz/s, and  $T_p = 2.5$   $\mu$ s, as defined in equation 1, and had a bandwidth of 900 MHz. This range was chosen because it included the passband of the all filters that were used for the experiment. The signal generator, however, was limited to a maximum bandwidth of 100 MHz. We circumvented this problem by redefining the probe signal to consider only the frequencies in or near the passband of the filter. This is known as the segmented probe. Using this assumption, we excited the filter with the segmented probe signal corresponding to the passband of that

particular filter to generate a partial reflected response. The partial response was then mapped to a full response and the gaps were filled with what the ideal response would have looked like outside the filter passband. The filter parameters were defined as follows:

- Filter 1: h(1)  $f_c = 900$  MHz,  $fbw = 27$  MHz,  $order=7$
- Filter 2: h(2)  $f_c = 900$  MHz,  $fbw = 36$  MHz,  $order=7$
- Filter 3: h(3)  $f_c = 900$  MHz,  $fbw = 45$  MHz,  $order=7$
- Filter 4: h(4)  $f_c = 500$  MHz,  $fbw = 25$  MHz,  $order=5$
- Filter 5: h(5)  $f_c = 465$  MHz,  $fbw = 5$  MHz,  $order=unknown$
- Filter 6: h(6)  $f_c = 465$  MHz,  $fbw = 5$  MHz,  $order=unknown$

The segmented probe signal used was

$$p^{*(i)}(t) = C \cos(\phi^{*(i)}(t)), \quad (10)$$

where

$$\dot{\phi}^{*(i)}(t) = \begin{cases} 2\pi f_0^{(i)} & , \quad 0 \leq t \leq \frac{T_{p^*}}{5} \\ 2\pi f_0^{(i)} + 2\pi K \left( t - \frac{T_{p^*}}{5} \right) & , \quad \frac{T_{p^*}}{5} \leq t \leq \frac{2T_{p^*}}{5} \\ 2\pi f_0^{(i)} + 2\pi K \left( \frac{T_{p^*}}{5} \right) & , \quad \frac{2T_{p^*}}{5} \leq t \leq \frac{3T_{p^*}}{5} \\ 2\pi f_0^{(i)} + 2\pi K \left( \frac{4T_{p^*}}{5} - t \right) & , \quad \frac{3T_{p^*}}{5} \leq t \leq \frac{4T_{p^*}}{5} \\ 2\pi f_0^{(i)} & , \quad \frac{4T_{p^*}}{5} \leq t \leq T_{p^*} \end{cases} \quad (11)$$

and the chirp rate was  $K = 120 \times 10^6$  MHz/s (the same as the original probe), with  $i$  denoting the filter number. The probe signal was input into the filter via a circulator and the reflected response was measured. A representation of this measurement system is shown in figure 13. This reflected response (figure 14) signal was then mapped into a synthetic reflected response based on the original 900-MHz probe (figure 15).

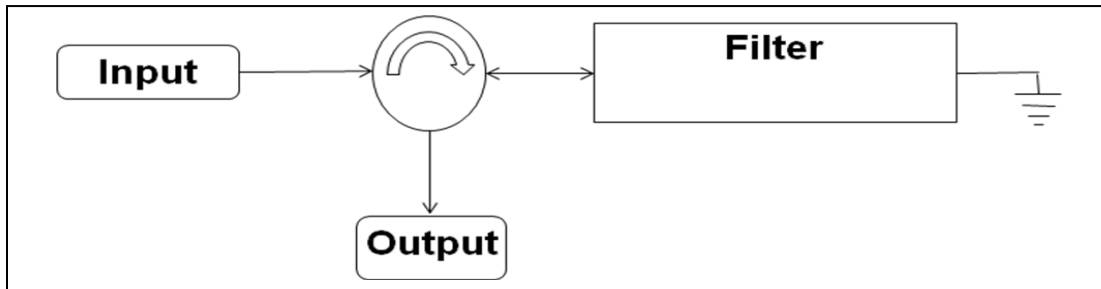


Figure 13. Experimental measurement system.



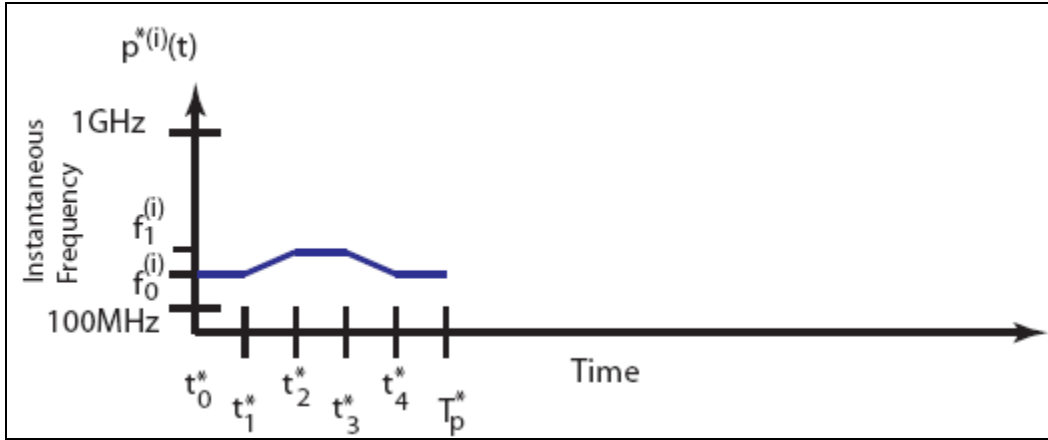


Figure 14. Frequency spectrum of excitation probe.

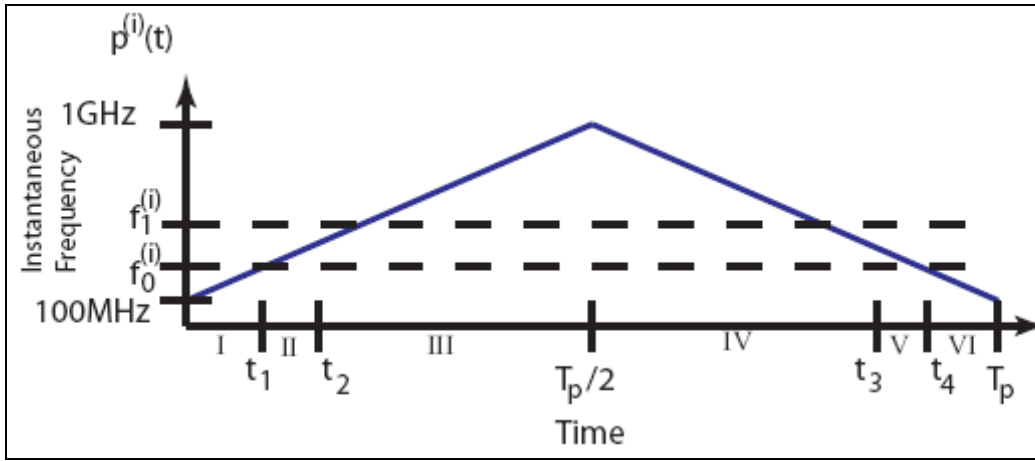


Figure 15. Frequency spectrum of mapped excitation.

Noise was added to the reflected response based on a target SNR. Once the target SNR was chosen, the noise power was determined relative to the power of the excitation probe signal. Features were extracted from the noise version of the response, grouped by SNR, and classified using a SVM classifier. The results from this classification are shown in figure 16.

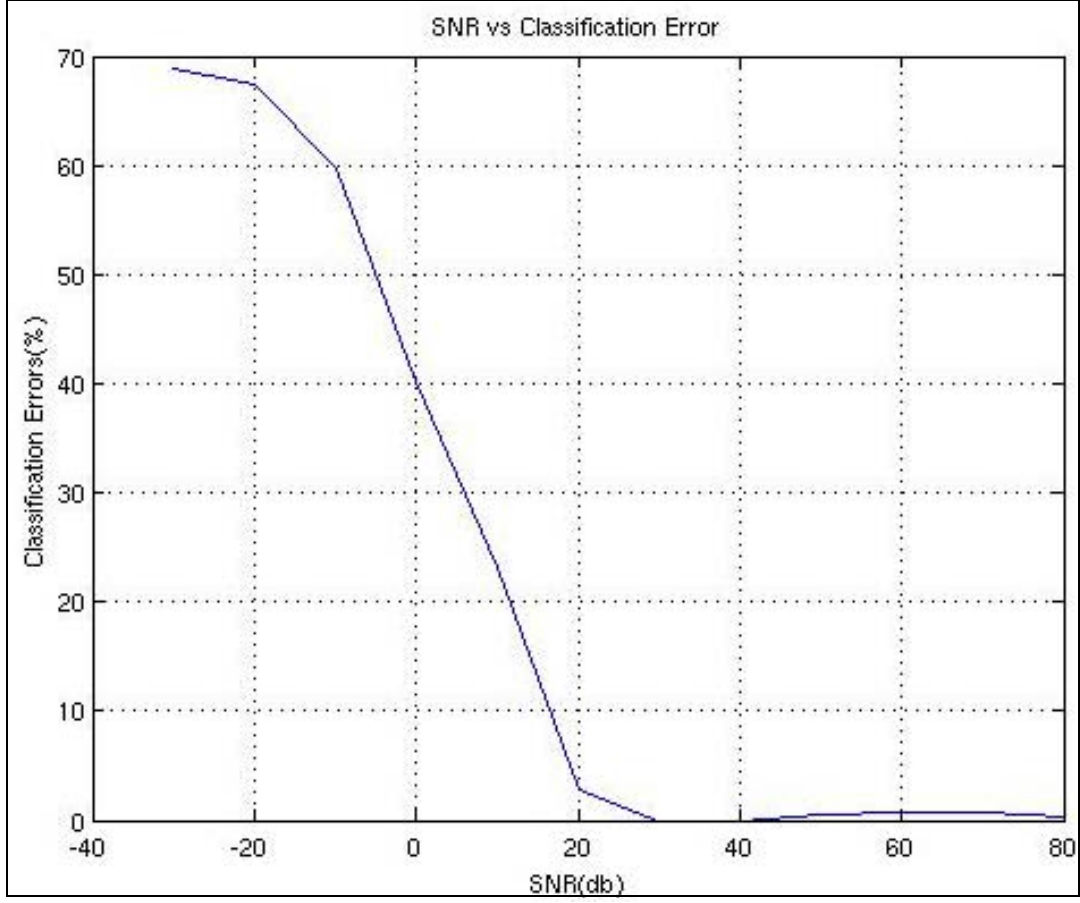


Figure 16. Result from SVM classifier segmented by SNR.

These results show that by using a relative small feature set we were able to obtain high classification accuracy at moderate SNRs. However, these results may have an inherent error due to the mapping and they do not account for the effect of a nonlinearity in the system. To address these issues, we measured the reflected response over a wide bandwidth with a nonlinearity present.

#### 4.6 Experimental Set up

Given the limitations presented by the hardware available at NCSU, we wanted to remove the need for mapping the reflected response by measuring the full reflected response from the system. For this experiment, we used a probe signal that had an initial starting frequency,  $f_0 = 100$  MHz; an end frequency,  $f_1 = 3100$  MHz; and  $T = 0.25$   $\mu$ s. This probe consisted of an up-chirp with instantaneous frequency:

$$\dot{\phi}(t) = 2\pi f_0 + 2\pi kt \quad (12)$$

We used the following filters in the experiments:

- Center Frequency: 1200 MHz – Band width: 120 MHz
- Center Frequency: 1860 MHz – Band width: 800 MHz
- Center Frequency: 660 MHz – Band width: 800 MHz
- Center Frequency: 247.5 MHz – Band width: 25 MHz.

These filters were excited by the probe signal with and without a pair of opposite diodes in parallel serving as the nonlinearity placed between the filter and the termination point. Only one response was measured for each filter-diode combination yielding eight measurement, four with the diode present and four without.

AWGN was then added to the measured reflected signal. The noise power was relative to the probe signal to achieve a target SNR. For this experiment, the target SNR (dBm) values were -60, -40, -20, -10, 0, 10, 20, 40, and 60. For each measured response, 500 noisy versions were created from each single response. In a manner similar to that used in section 3.2, the responses from the filter were grouped into supersets based on filter only and filter + diode. The filter only case included all cases where a filter was present. For example, the filter 1 class included both the cases where the nonlinearity was and was not present and thus yielded 1,000 noisy responses. The filter + diode case treated each type of response as a different class and resulted in 500 noisy responses in each class.

By adding noise, we can build a test and training set for the SVM classifier. From each member of the training and testing sets, features were extracted in the manner described in section 4.4. The features included center frequency, bandwidth, and a 34-point sample of the passband of the filter yielding a 36-point feature vector. An SVM classifier was used for classification. The results are shown in table 6.

Table 6. Resulting classification accuracies determined by the SVM for Experiment 2.

<b>SNR (dBm)</b>	<b>Filter + Diode</b>	<b>Filter Only</b>
-60	12.05%	26.06%
-40	99.50%	100%
-20	100%	100%
-10	100%	100%
0	100%	100%
10	100%	100%
20	100%	100%
40	100%	100%
60	100%	100%

Initial analysis of this data infers that the mapping process shifts the classification curve to the right, achieving comparable classification results when SNR levels are reduced by 40–60 dB.

---

## **5. Future Work**

---

While the diode model used provides a foundation for modeling nonlinearities, it still warrants further investigation. We noticed that the amplitude plays a major role in the response of the nonlinearity; this parameter should be looked at in more detail. When combined with a filter, it would be of interest to observe whether the shape or the amplitude of the response plays a more significant role in classification. Also, since the filter seems to be the dominate feature in both sets of experiments, a tiered classification system should be explored. This type of system would classify based on filter first, followed by a diode-based classification.

---

## 6. References

---

1. Federal communication commission rules and regulations. <http://www.fcc.gov/oet/info/rules/> <<http://www.fcc.gov/oet/info/rules/> (accessed December 2009).
2. RTCA SC-202, DO-294, Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDs) on Aircraft, October 19, 2004.
3. Ely, J. J. Electromagnetic Interference to Flight Navigation and Communication Systems: New Strategies in the Age of Wireless. *AIAA Atmospheric Flight Mechanics Conference and Exhibit*, San Francisco, CA, 15–18 Aug 2005.
4. Woods, R.; Ely, J. J.; Vahala, L. Detecting the Use of Intentionally Transmitting Personal Electronic Devices Onboard Commercial Aircraft. *IEEE Electromagnetic Compatibility Meeting*, Boston, MA, 18–22 Aug 2003.
5. Martone, A. F.; Delp, E. J. Forensic Characterization of RF Circuits. Ph.d. Thesis, Purdue University, West Lafayette, IN, Dec 2007.
6. Lin, I.; McKinney, J.; Weiner, A. Shaping the Power Spectrum of Ultrawideband Radio-frequency Signals. *IEEE Transactions on Microwave Theory and Techniques* **December 2006**, 54 (12), 4247–4255.
7. Chang, C. C.; Lin, C. J. *LIBSVM: a Library for Support Vector Machines*, 2001, <http://www.csie.ntu.edu.tw/~cjlin/libsvm>.
8. King-Smith, D.; Mikkilineni, A. K.; Gelfand, S.; E. J. D. III. RF Device Forensics Using Passband Filter Analysis. *Proceedings of the SPIE International Conference on Media Forensics and Security*, vol. 7254, San Jose, CA, January 2009, p 725419.

---

## List of Symbols, Abbreviations, and Acronyms

---

AWGN	Additive White Gaussian Noise
BC	Bayesian classifier
BT	Binary Tree
FCC	Federal Communications Commission
HP	Hewlett-Packard
IF	intermediate frequency
I-V	current versus applied voltage
K-NN	K-Nearest Neighbors
NCSU	North Carolina State University
PEDs	Portable Electronic Devices
PSD	power spectral density
PW	Parzen Window
R-G	recombination-generation
SNR	signal-to-noise ratio
SVM	Support Vector Machines
T-PEDs	transmitting PEDs

NO. OF COPIES	ORGANIZATION
1 ELECT	ADMNSTR DEFNS TECHL INFO CTR ATTN DTIC OCP 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218
1 CD	DARPA ATTN IXO S WELBY 3701 N FAIRFAX DR ARLINGTON VA 22203-1714
1	OFC OF THE SECY OF DEFNS ATTN ODDRE (R&AT) THE PENTAGON WASHINGTON DC 20301-3080
1	US ARMY RSRCH DEV AND ENGRG CMND ARMAMENT RSRCH DEV AND ENGRG CTR ARMAMENT ENGRG AND TECHNLGY CTR ATTN AMSRD AAR AEF T J MATTS BLDG 305 ABERDEEN PROVING GROUND MD 21005-5001
1	PM TIMS, PROFILER (MMS-P) AN/TMQ-52 ATTN B GRIFFIES BUILDING 563 FT MONMOUTH NJ 07703
1	US ARMY INFO SYS ENGRG CMND ATTN AMSEL IE TD A RIVERA FT HUACHUCA AZ 85613-5300
1	COMMANDER US ARMY RDECOM ATTN AMSRD AMR W C MCCORKLE 5400 FOWLER RD REDSTONE ARSENAL AL 35898-5000
1	US GOVERNMENT PRINT OFF DEPOSITORY RECEIVING SECTION ATTN MAIL STOP IDAD J TATE 732 NORTH CAPITOL ST NW WASHINGTON DC 20402

NO. OF COPIES	ORGANIZATION
1	PURDUE UNIV SCHOOL OF ELEC AND COMPUTER ENGRG ELEC ENGRG BLDG ATTN D KING-SMITH 465 NORTHWESTERN AVE WEST LAFAYETTE IN 47907-2035
1	US ARMY RSRCH LAB ATTN RDRL CIM G T LANDFRIED BLDG 4600 ABERDEEN PROVING GROUND MD 21005-5066
21	US ARMY RSRCH LAB ATTN IMNE ALC HRR MAIL & RECORDS MGMT ATTN RDRL CIM L TECHL LIB ATTN RDRL CIM P TECHL PUB ATTN RDRL SER U A MARTONE (10 COPIES) ATTN RDRL SER U A SULLIVAN ATTN RDRL SER U F KOENIG ATTN RDRL SER U J COSTANZA ATTN RDRL SER U K KAPPRA ATTN RDRL SER U K RANNEY ATTN RDRL SER U K SHERBONDY ATTN RDRL SER U L NGUYEN ATTN RDRL SER U M RESSLER ADELPHI MD 20783-1197

TOTAL: 31 (29 HCS, 1 CD, 1 ELECT)

INTENTIONALLY LEFT BLANK.